Polityka publiczna w zakresie ochrony cyberprzestrzeni w UE i państwach członkowskich

Chmielewski, Zbigniew

Veröffentlichungsversion / Published Version
Zeitschriftenartikel / journal article

Zbigniew Chmielewski

Polityka publiczna w zakresie ochrony cyberprzestrzeni w UE i państwach członkowskich

Streszczenie

Celem artykułu jest przedstawienie najważniejszych regulacji i działań podejmowanych przez Unię Europejską w ramach polityki publicznej ukierunkowanej na ochronę cyberprzestrzeni oraz dokonanie kompleksowej analizy porównawczej podstawowych regulacji dotyczących cyberbezpieczeństwa funkcjonujących w państwach członkowskich UE. W artykule zaprezentowano katalog zagadnień, które powinny się znajdować w kręgu zainteresowania polityki publicznej w zakresie cyberbezpieczeństwa, co pozwoliło przeanalizować, czy zostały one odzwierciedlone w istniejących regulacjach utworzonych na poziomie Unii Europejskiej i w jaki sposób. Opierając się na przeprowadzonych w 2015 r. przez BSA – The Software Alliance badaniach i innych dostępnych źródłach, przeanalizowano przygotowanie państw członkowskich UE do zapewnienia bezpieczeństwa w cyberprzestrzeni. Szczególną uwagę poświęcono przy tym Polsce, odnosząc się do założeń nowej strategii cyberbezpieczeństwa dla Rzeczypospolitej Polskiej, opracowanych przez Ministerstwo Cyfryzacji i opublikowanych w lutym 2016 r.

Słowa kluczowe: polityka publiczna, cyberbezpieczeństwo, cyberprzestrzeń, Unia Europejska, państwa członkowskie

Public policy on cybersecurity in the E.U. and E.U. Member States

Abstract

The purpose of this article is to provide a detailed overview of the essential measures and regulations implemented by the European Union within the framework of its public policy on cybersecurity and make a comprehensive comparative analysis of the cybersecurity capabilities in E.U. Member States and their national strategies in this area. This article highlights multiple issues that should be the center of attention in regard to public policy on cybersecurity, which made it possible to evaluate the compliance of the existing

regulations passed by the E.U. policy makers and the way it was approached. Based on the 2015 Software Alliance (BSA) survey and other available sources an analysis was made to evaluate the readiness of E.U. Member States to ensure security in cyberspace. Special attention was paid to "The Assumptions of Cybersecurity Strategy of the Republic of Poland", developed by the Ministry of Digitisation and published in February 2016.

Keywords: public policy, cybersecurity, cyberspace, the European Union, E.U. Member States

Zakres przedmiotowy niniejszego artykułu obejmuje regulacje i inicjatywy Unii Europejskiej wynikające z prowadzonej polityki publicznej ukierunkowanej na ochronę jej cyberprzestrzeni oraz ich odzwierciedlenie na poziomie krajowym w państwach członkowskich. Ze względu na ograniczenia powodowane objętością jedynie w minimalnym zakresie w artykule przedstawiono instytucje i organa ustanowione na szczeblu Unii Europejskiej, których zadania związane są z różnymi aspektami zapewnienia bezpieczeństwa cybernetycznego – niemniej warto odnotować istnienie takich organów, jak ENISA (European Network and Information Security Agency), CERT-EU, czyli Centrum Reagowania na Incydenty Komputerowe dla instytucji Unii Europejskiej, ustanowione na stałe po rocznym okresie pilotażowym w 2012 r. i koordynujące obecnie działania krajowych CERT, oraz utworzone w 2013 r. w strukturach Europolu Europejskie Centrum ds. Walki z Cyberprzestępczością (European Cybercrime Centre, EC3). W celu uniknięcia fragmentaryczności w podejściu obszar badań zawężono do ram wyznaczonych na podstawie analizy anglojęzycznej literatury przedmiotu. Pomimo powiązania niektórych aspektów strategii w zakresie bezpieczeństwa cybernetycznego z cyberobroną, tym zagadnieniom nie poświęca się uwagi w szerszym ujęciu.

Definicje pojęć cyberprzestrzeni i cyberbezpieczeństwa

Pojęcie „cyberprestrzeń" (*cyberspace*) wywodzi się etymologicznie z cybernetyki, która, zgodnie z intencją jej twórcy N. Wienera, na co wskazuje P. Sienkiewicz[1], jest nauką o sterowaniu i komunikowaniu w obiektach (systemach) dowolnej natury. Równocześnie jednak ma ono beletrystyczny wydźwięk, albowiem zostało wymyślone przez amerykańskiego pisarza W. Gibsona i użyte po raz pierwszy w jego powieściach z gatunku *science fiction* opublikowanych w latach 1982 i 1984. Jak

[1] P. Sienkiewicz, *Analiza systemowa zagrożeń dla cyberprzestrzeni*, „Automatyka" 2009, nr 2(13), s. 584.

odnotowuje R. Białoskórski[2], powieści *Burning Chrome* i *Neuromancer* przedstawiają wygenerowany przez komputer świat immersyjnej, wirtualnej rzeczywistości określany matrycą. Według M. Berdel-Dudzińskiej[3], W. Gibson, nazywając wirtualną, trójwymiarową przestrzeń elektronicznego medium komunikacyjnego królestwem przestrzennych paradoksów, równocześnie określił cyberprzestrzeń jako zbiorową halucynację przeżywaną przez jej użytkowników.

Analiza istotnych cech cybernetycznej przestrzeni pozwala rozpatrywać cybernetykę sieci jako technosystem globalnej komunikacji społecznej, który charakteryzuje interaktywność i multimedialność[4]. Specyfika cyberprzestrzeni stwarza wiele trudności w dokładnym zdefiniowaniu tego pojęcia. Jednakże na podstawie prowadzonych analiz, obserwacji i badań nad cyberprzestrzenią określono charakterystyczne jej cechy, rzutujące na działania w jej ramach, z których do najważniejszych można zaliczyć aterytorialność cyberprzestrzeni, sprawiającą, że wszelka aktywność jakiegokolwiek podmiotu w jej obszarze nie ma żadnych ograniczeń przestrzennych w postaci np. granicy geograficznej, politycznej itd., anonimowość podmiotów w niej operujących i, wreszcie, systemowość i szeroki zasięg, będące konsekwencją stale powiększającej się gęstości powiązań konstytuujących cyberprzestrzeń[5].

Jedną z najbardziej znanych i powszechnie cytowanych jest definicja cyberprzestrzeni sformułowana przez Departament Obrony USA na potrzeby powołania jednolitego słownika terminologii wojskowej oraz powiązanej, zgodnie z którą cyberprzestrzeń to globalna domena środowiska informacyjnego, składająca się z współzależnych sieci tworzonych przez infrastrukturę technologii informacyjnej (IT) oraz zawartych w nich danych, włączając Internet, sieci telekomunikacyjne, systemy komputerowe, a także osadzone w nich procesory i kontrolery[6]. W polskojęzycznej literaturze przedmiotu istnieje wiele definicji tego pojęcia. Zgodnie z definicją zaproponowaną przez R. Tadeusiewicza[7], cyberprzestrzenią jest ogół narzędzi sprzętowych i programowych związanych z technikami gromadzenia, przetwarzania, przesyłania i udostępniania informacji, wykorzystywanych przez ludzi do pozyskiwania wiedzy

[2] R. Białoskórski, *Cyberzagrożenia w środowisku bezpieczeństwa XXI wieku: Zarys problematyki*, Wyższa Szkoła Cła i Logistyki, Warszawa 2011, s. 13.

[3] M. Berdel-Dudzińska, *Pojęcie cyberprzestrzeni we współczesnym polskim porządku prawnym*, „Przegląd Prawa Publicznego" 2012, nr 2, s. 23.

[4] P. Sienkiewicz, H. Świeboda, *Analiza systemowa bezpieczeństwa cyberprzestrzeni państwa*, „Polskie Stowarzyszenie Zarządzania Wiedzą", Seria: Studia i Materiały, 2010, nr 33, s. 28.

[5] R. Reczkowski, A. Skiba, *Bezpieczeństwo państwa w kontekście zagrożeń z cyberprzestrzeni*, w: *Innowacje i synergia w Siłach Zbrojnych RP, t. 1*, red. nauk. A. Lis, R. Reczkowski, Centrum Doktryn i Szkolenia Sił Zbrojnych im. gen. broni Władysława Sikorskiego, Bydgoszcz 2012, s. 124–128.

[6] J. Wasilewski, *Zarys definicyjny cyberprzestrzeni*, „Przegląd Bezpieczeństwa Wewnętrznego" 2013, nr 9, s. 227.

[7] R. Tadeusiewicz, *Zagrożenia w cyberprzestrzeni*, „Nauka" 2010, nr 4, s. 32.

oraz do komunikacji z innymi ludźmi. Warto nadmienić, że w definicji tej równocześnie podkreśla się, iż najważniejszym, chociaż nie jedynym, składnikiem cyberprzestrzeni jest obecnie Internet. Przytoczona definicja jest definicją dwuaspektową, na co wskazują J. Rzucidło i J. Węgrzyn[8], albowiem ujmuje cyberprzestrzeń nie tylko jako pewną infrastrukturę techniczną, ale także obszar relacji ludzi z tą infrastrukturą, jak i interakcje między ludźmi związane z jej wykorzystaniem.

Definicja prawna pojęcia cyberprzetrzeni w polskim ustawodawstwie znajduje się w trzech ustawach: Ustawie z dnia 21 czerwca 2002 r. o stanie wyjątkowym[9], Ustawie z dnia 29 sierpnia 2002 r. o stanie wojennym oraz o kompetencjach Naczelnego Dowódcy Sił Zbrojnych i zasadach jego podległości konstytucyjnym organom Rzeczypospolitej Polskiej[10], w Ustawie z dnia 18 kwietnia 2002 r. o stanie klęski żywiołowej[11] (wspomniane ustawy zostały uzupełnione o przepisy dotyczące cyberprzestrzeni, wprowadzone w życie z dniem 2 listopada 2011 r., zgodnie z Ustawą z dnia 30 sierpnia 2011 r. o zmianie ustawy o stanie wojennym oraz o kompetencjach Naczelnego Dowódcy Sił Zbrojnych i zasadach jego podległości konstytucyjnym organom Rzeczypospolitej Polskiej oraz niektórych innych ustaw[12]).

W definicji pojęcia cyberprzestrzeni wprowadzonej do porządku prawnego podkreśla się, że przez cyberprzestrzeń należy rozumieć przestrzeń przetwarzania i wymiany informacji tworzoną przez systemy teleinformatyczne, określone w art. 3 pkt. 3 Ustawy z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne[13], wraz z powiązaniami pomiędzy nimi oraz relacjami z użytkownikami (systemami teleinformatycznymi są zespoły współpracujących ze sobą urządzeń informatycznych i oprogramowania zapewniające przetwarzanie, przechowywanie, a także wysyłanie i odbieranie danych przez sieci telekomunikacyjne za pomocą właściwego dla danego rodzaju sieci telekomunikacyjnego urządzenia końcowego przeznaczonego do podłączenia bezpośrednio lub pośrednio do zakończeń sieci[14]).

---

[8] J. Rzucidło, J. Węgrzyn, *Stany nadzwyczajne w sytuacji szczególnego zagrożenia państwa w cyberprzestrzeni*, „Przegląd Prawa Konstytucyjnego" 2015, nr 5(27), s. 142.

[9] Zob. Ustawa z dnia 21 czerwca 2002 r. o stanie wyjątkowym, Dz. U. 2002, nr 117, poz. 985, z późn. zm.

[10] Zob. Ustawa z dnia 29 sierpnia 2002 r. o stanie wojennym oraz o kompetencjach Naczelnego Dowódcy Sił Zbrojnych i zasadach jego podległości konstytucyjnym organom Rzeczypospolitej Polskiej, Dz. U. 2002, nr 156, poz. 1301, z późn. zm.

[11] Zob. Ustawa z dnia 18 kwietnia 2002 r. o stanie klęski żywiołowej, Dz. U. 2002, nr 62, poz. 558, z późn. zm.

[12] Zob. Ustawa z dnia 30 sierpnia 2011 r. o zmianie ustawy o stanie wojennym oraz o kompetencjach Naczelnego Dowódcy Sił Zbrojnych i zasadach jego podległości konstytucyjnym organom Rzeczypospolitej Polskiej oraz niektórych innych ustaw, Dz. U. 2011, nr 222, poz. 1323.

[13] Zob. Ustawa z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne, Dz. U. 2005, nr 64, poz. 565, z późn. zm.

[14] Przyp. autora.

Analizując najistotniejsze cechy legalnej definicji, J. Wasilewski[15] wskazuje na fakt, iż definicja ta wprowadza ideę jednej cyberprzestrzeni, będącej wydzielonym logicznie obszarem – cyfrową domeną przetwarzania oraz wymiany informacji. Przestrzeń ta, mająca charakter ponadnarodowy, jest tworzona przez systemy teleinformatyczne połączone za pośrednictwem sieci telekomunikacyjnych, w tym sieci, których elementy infrastrukturalne są zlokalizowane na terenie innych państw. Działanie w cyberprzestrzeni nie ogranicza się wyłącznie do wymiany informacji. Może ono również polegać na samym ich wytwarzaniu, modyfikowaniu czy po prostu odczytywaniu. Tak więc i te operacje są dokonywane na gruncie domeny cyfrowej. W definicji tej, jak odnotowuje ponadto J. Wasilewski[16], wskazując także na wzajemne relacje systemów z użytkownikami, podkreślono swojego rodzaju dwustronne powiązanie działań w cyberprzestrzeni z działaniami w „fizycznej" rzeczywistości (rzeczywistym świecie) oraz ich wzajemne konsekwencje.

Przestrzeń wirtualna, cyfrowa może być też traktowana jako terytorium określonego państwa[17]. W Polsce dokument pt. *Polityka ochrony cyberprzestrzeni Rzeczypospolitej Polskiej*, przyjęty w 2013 r. przez Ministerstwo Administracji i Cyfryzacji oraz Agencję Bezpieczeństwa Wewnętrznego[18], wprowadził definicję pojęcia cyberprzestrzeni Rzeczypospolitej Polskiej, w myśl której jest nią cyberprzestrzeń w obrębie terytorium państwa polskiego i poza jego terytorium, w miejscach gdzie funkcjonują przedstawiciele RP (placówki dyplomatyczne, kontyngenty wojskowe). W przyjętej w 2015 r. *Doktrynie cyberbezpieczeństwa Rzeczypospolitej Polskiej*[19] definicja cyberprzestrzeni pozostaje bez zmian.

Termin „cyberbezpieczeństwo" wywodzi się z terminu „bezpieczeństwo informacyjne", jednakże jest używany w odniesieniu do szerszego zakresu zagadnień, związanych również z bezpieczeństwem narodowym[20]. Jednej uniwersalnej definicji cyberbezpieczeństwa nie ma. W dokumencie pt. *Strategia bezpieczeństwa cybernetycznego Unii Europejskiej: otwarta, bezpieczna i chroniona cyberprzestrzeń*, przedstawionym przez Komisję Europejską w dniu 7 lutego 2013 r.[21], stwierdza się, iż bezpieczeństwo cybernetyczne ogólnie odnosi się do zabezpieczeń i działań, które

[15] J. Wasilewski, op.cit, s. 231.

[16] Ibidem.

[17] J. Skrzypczak, *Polityka ochrony cyberprzestrzni RP*, „Przegląd Strategiczny" 2014, nr 7, s. 133.

[18] Zob. *Polityka ochrony cyberprzestrzeni Rzeczypospolitej Polskiej*, Ministerstwo Administracji i Cyfryzacji – Agencja Bezpieczeństwa Wewnętrznego, Warszawa 2013, s. 5.

[19] Zob. *Doktryna cyberbezpieczeństwa Rzeczypospolitej Polskiej*, Warszawa 2015, s. 7.

[20] *Cybersecurity in the European Union and Beyond: Exploring the Threats and Policy Responses, Directorate – General for Internal Policies*, European Union, Brussels 2015, s. 13.

[21] Zob. Wspólny komunikat Komisji do Parlamentu Europejskiego, Rady, Europejskiego Komitetu Ekonomiczno-Społecznego i Komitetu Regionów, *Strategia bezpieczeństwa cybernetycznego Unii Europejskiej* (JOIN (2013) 1 final z 7.2.2013), s. 3.

mogą być wykorzystywane do ochrony domeny cybernetycznej, zarówno cywilnej, jak i wojskowej, przed tymi zagrożeniami, które dotyczą jej współzależnych sieci i infrastruktury informatycznej oraz które mogą te sieci oraz tę infrastrukturę uszkodzić.

Bezpieczeństwo cybernetyczne polega na działaniach mających na celu zachowanie dostępności i integralności sieci i infrastruktury oraz zachowanie poufności zawartych w nich informacji. Można też odwołać się do dwóch definicji proponowanych przez Narodową Inicjatywę w zakresie Karier i Studiów w Dziedzinie Cyberbezpieczeństwa (National Initiative for Cybersecurity Careers and Studies, NICCS), czyli jednostkę zarządzaną przez wydział edukacji i świadomości cyberbezpieczeństwa znajdujący się w strukturze Departamentu Bezpieczeństwa Wewnętrznego Urzędu Cyberbezpieczeństwa i Komunikacji Rządu Federalnego USA. Zgodnie z wąską definicją[22], cyberbezpieczeństwem jest wynik ukierunkowanej działalności lub procesu bądź stan, kiedy systemy informacyjne lub komunikacyjne oraz informacja zawarta w nich są zabezpieczone czy chronione przed uszkodzeniem, nieautoryzowanym użyciem, modyfikacją bądź wykorzystaniem.

Oprócz wąskiej definicji opracowano także poszerzoną[23], ujmującą cyberbezpieczeństwo jako strategię, politykę i normy dotyczące zarówno bezpieczeństwa cyberprzestrzeni, jak i działania w niej, obejmujące z jednej strony pełen zakres czynności ukierunkowanych na redukcję zagrożeń, zmniejszenie podatności na nie i odstraszanie, międzynarodowe zaangażowanie, reagowanie na zdarzenia, zaś z drugiej – elastyczną politykę prewencyjną, uwzględniającą odpowiednie operacje w sieci komputerowej, zapewnienie informacji, działania organów ścigania, dyplomacji, wojska, służb wywiadowczych, odnoszące się do bezpieczeństwa i stabilności globalnej infrastruktury informacyjnej i komunikacyjnej.

Cyberbezpieczeństwo jako przedmiot zainteresowania polityki publicznej na forum Unii Europejskiej

Cyberbezpieczeństwo znajduje się w centrum zainteresowania polityki publicznej od ćwierć wieku. Wystarczy bowiem nadmienić, że Narodowa Rada ds. Badań (National Research Council) jeszcze w 1991 r. stwierdziła w opracowaniu pt. *Komputery w niebezpieczeństwie: bezpieczne przetwarzanie danych w epoce informacyjnej*, iż Stany Zjednoczone coraz bardziej są uzależnione od komputerów, kontrolujących

[22] Por. C. Vishik, M. Matsubara, A. Plonk, *Key Concepts in Cyber Security: Towards a Common Policy and Technology Context for Cyber Security Norms*, w: *International Cyber Norms: Legal, Policy & Industry Perspectives*, A.-M. Maria Osula, H. Rõigas (Eds.), NATO CCD COE Publications, Tallinn 2016, s. 221.

[23] Ibidem, s. 221–222.

dostawę energii, zarządzających komunikacją, lotnictwem i usługami finansowymi oraz wykorzystywanych do przechowywania wirtualnych informacji, poczynając od danych medycznych i kończąc na rejestrach karanych. Rada odnotowała równocześnie, że komputery mogą być narażone na celowe ataki, dzięki którym nowoczesny złodziej może ukraść więcej, korzystając z komputerów niż z pistoletu, zaś jutrzejszy terrorysta będzie mógł wyrządzić więcej szkód, używając klawiatury niż w wyniku użycia bomby[24]. Poza wszelką wątpliwość, Stany Zjednoczone mają najdłuższe doświadczenie w dziedzinie cyberbezpieczeństwa. Analizując, jakie zagadnienia dotyczące bezpieczeństwa cyberprzestrzeni znajdują się w centrum uwagi na forum Unii Europejskiej, warto zatem odnieść się (w celu dokonania porównań) do katalogu zagadnień, które powinny być regulowane przez politykę publiczną w zakresie cyberbezpieczeństwa, opracowanego przez amerykańskich autorów zajmujących się tą problematyką. Katalog ten jest dosyć obszerny i obejmuje:

- kwestie związane z wielopłaszczyznowym i wielopodmiotowym zarządzaniem (*governance*) cyberprzestrzenią (neutralność sieciowa na rynku komunikacji elektronicznej, przydzielanie nazw i adresów w Internecie, prawa autorskie i znaki towarowe, niechciana korespondencja e-mailowa),
- kwestie związane z użytkownikami cyberprzestrzeni: działaniem reklam zawierających złośliwe oprogramowanie (*malvertising*), podawaniem się za kogoś innego (*impersonation*), odpowiednim korzystaniem, cyberprzestępczością, geolokalizacją, prywatnością,
- zagadnienia związane z cyberkonfliktami (kradzież własności intelektualnej, cyberszpiegostwo, cybersabotaż, cybernetyczne działania wojenne – *cyber warfare*),
- problemy związane z infrastrukturą cyberprzestrzeni,
- szczegółowe problemy zarządzania cyberprzestrzenią (m.in. odpowiedzialność za powierzone dane, zarządzanie ryzykiem, certyfikowanie zawodów, zasady bezpieczeństwa, badania i rozwój)[25].

Bardzo podobnie obszary zainteresowania polityki publicznej w tym zakresie definiowane są przez takich autorów, jak D. Clark, T. Berson i H.S. Lin[26], którzy wskazują, iż nieelastyczne regulacje mające na celu zapewnienie cyberbezpieczeństwa mogą przyczyniać się do wywoływania wielu niekorzystnych konsekwencji.

Charakteryzując szczegółowo pierwszy z przedstawionych pięciu bloków zagadnieniowych, warto zwrócić uwagę na wystosowany w lutym 2014 r. przez Komisję

[24] Por. D. Clark, T. Berson, H.S. Lin (Eds.), *At the Nexus of Cybersecurity and Public Policy: Some Basic Concepts and Issues*, The National Academies Press, Washington 2014, s. 10–11.

[25] Por. J.L. Bayuk, J. Healey, P. Rohmeyer, M.H. Sachs, J. Schmidt, J. Weiss, *Cyber Security Policy Guidebook*, John Wiley & Sons Inc., Hoboken, New Jersey 2012, s. 89.

[26] D. Clark, T. Berson, H.S. Lin (Eds.), op.cit., s. 13–15.

Europejską Komunikat Komisji do Parlamentu Europejskiego, Rady, Europejskiego Komitetu Ekonomiczno-Społecznego i Komitetu Regionów dotyczący polityki wobec Internetu i zarządzania Internetem oraz roli Europy w kształtowaniu przyszłości zarządzania Internetem[27]. W kwestii modelu zarządzania Internetem w komunikacie zostało zaprezentowane stanowisko popierane na różnych forach globalnych przez Unię Europejską i Stany Zjednoczone, uznające, że najbardziej optymalny jest model wielopłaszczyznowego i wielopodmiotowego zarządzania (*governance*), w którym pozycji dominującej nie ma żaden z podmiotów dopuszczonych do decydowania o kształcie funkcjonowania sieci. Komisja Europejska uważa również, że procesowi *governance* powinny podlegać także kwestie techniczne dotyczące zarówno protokołów internetowych, jak i innych technologii informacyjnych[28]. Jak podkreśla się w komunikacie, szczegóły techniczne dotyczące protokołów internetowych i specyfikacje innych technologii informacyjnych mogą wywoływać znaczące skutki w zakresie polityki publicznej. Mogą one oddziaływać na prawa człowieka, takie jak prawo użytkowników do ochrony danych oraz do bezpieczeństwa, dostęp do zróżnicowanych zasobów wiedzy i informacji oraz wolność słowa w Internecie. Normy techniczne kształtujące Internet mają znaczenie również dla innych zainteresowanych stron, w tym dla przedsiębiorców prowadzących działalność gospodarczą w Internecie, których potrzeby w zakresie bezpieczeństwa także należy wziąć pod uwagę[29].

W aktualnym stanie prawnym zarówno w Unii Europejskiej, jak i w Polsce wciąż brakuje definicji legalnej pojęcia neutralności sieciowej[30]. Komisja Europejska rozpatruje neutralność sieciową zgodnie z zasadą prymatu konkurencji oraz z uwzględnieniem podstawowych praw obywateli Unii Europejskiej, takich jak: poszanowanie życia prywatnego, ochrona danych osobowych, wolność wypowiedzi oraz wolność prowadzenia działalności biznesowej. Zdaniem Komisji Europejskiej, znaczenie różnych problemów związanych z neutralnością sieciową zależy od stopnia konkurencji na rynku.

Konkurencja ma gwarantować otwartość Internetu oraz poprawne funkcjonowanie i współdziałanie sieci z użytkownikiem. Dlatego naruszenie zasad uczciwej konkurencji,

---

[27] Zob. Komunikat Komisji do Parlamentu Europejskiego, Rady, Europejskiego Komitetu Ekonomiczno-Społecznego i Komitetu Regionów, *Polityka wobec Internetu i zarządzanie Internetem: Rola Europy w kształtowaniu przyszłości zarządzania Internetem* (COM (2014) 72 final z 12.2.2014).

[28] A. Jaskiernia, M. Głowacki, *Unia Europejska i Rada Europy a kwestie ochrony praw człowieka w Internecie. Europejskie standardy zarządzania Internetem*, „Studia Medioznawcze" 2014, nr 3(58), s. 148.

[29] Zob. Komunikat Komisji do Parlamentu Europejskiego, Rady, Europejskiego Komitetu Ekonomiczno-Społecznego i Komitetu Regionów, *Polityka wobec Internetu i zarządzanie Internetem: Rola Europy*…, op.cit., s. 9–10.

[30] A. Nałęcz, *Neutralność sieciowa*, „Internetowy Kwartalnik Antymonopolowy i Regulacyjny" 2015, nr 6(4), s. 27.

jak praktyki oligopolistyczne, stwarzanie barier w dostępie do rynku, a także asymetria informacji, prowadzą do zakłócenia zasad neutralności sieciowej[31]. Wiele wyjaśnia niezwykle prosty opis stosowany przez Organ Europejskich Regulatorów Łączności Elektronicznej (BEREC), zgodnie z którym neutralność sieciowa oznacza, że wszystkie elektroniczne komunikaty przesyłane w sieci Internet traktowane są jednakowo. Innymi słowy, każdy komunikat podlega takiemu samemu traktowaniu niezależnie od jego treści, wykorzystanej aplikacji lub usługi, urządzenia i adresu nadawcy lub odbiorcy[32]. W Unii Europejskiej niektóre kwestie związane z neutralnością sieciową zostały uwypuklone w pakiecie regulacyjnym przyjętym w 2009 r.[33].

Unia Europejska już pod koniec lat 90. XX w. była aktywnym i wpływowym uczestnikiem międzynarodowych dyskusji toczonych wówczas wokół utworzenia Internetowej Korporacji ds. Nadawania Nazw i Numerów (Internet Corporation for Assigned Names and Numbers, ICANN) oraz zdefiniowania celów tej organizacji[34]. Jest to organizacja sektora prywatnego o charakterze non-profit, odpowiedzialna za centralną administrację domenami internetowymi. Instytucja ta powstała, aby przejąć zarządzanie systemem DNS[35] od amerykańskiego rządu na rzecz globalnej społeczności w celu zwiększenia konkurencji i ułatwienia międzynarodowego uczestnictwa w zarządzaniu tym systemem. Funkcjonuje ona na podstawie porozumień z Departamentem Handlu Stanów Zjednoczonych Ameryki, a pierwszym dokumentem w tym zakresie było *Memorandum of Understanding Between ICANN and U.S. Department of Commerce* z 25.11.1998 r[36]. W 2005 r. rząd USA zobowiązał się do współpracy ze wspólnotą międzynarodową w kwestiach zagrożenia interesu publicznego, które dotyczą zarządzania krajowymi domenami najwyższego poziomu (ccTLD). Zobowiązanie to nie zostało jednak jeszcze w pełni zrealizowane. W komunikacie z 2009 r. Komisja Europejska zwróciła uwagę na niekompletność internacjonalizacji głównych funkcji oraz organizacji Internetu. Od 2009 r. ICANN podejmuje kroki w tym kierunku, jednakże status prawny ICANN na mocy prawa stanu Kalifornia ze stosunkiem umownym z jednym państwem nie uległ zmianie. Wyłączny związek ICANN z jednym rządem – o którym świadczy potwierdzenie zobowiązań – wywodzi się z początkowego okresu Internetu i musi w dobie Internetu

[31] F. Kamiński, *Problematyka neutralności sieciowej w Unii Europejskiej (zarys)*, „Telekomunikacja i Techniki Informacyjne" 2011, nr 3–4, s. 25.

[32] A. Nałęcz, op.cit., s. 27.

[33] F. Kamiński, op.cit., s. 25.

[34] Zob. Komunikat Komisji do Parlamentu Europejskiego i Rady, *Zarządzanie Internetem*: *kolejne działania* (COM (2009) 277 końcowy z 18.6.2009), s. 4–5.

[35] DNS – jest to skrót od Domain Name System, co w tłumaczeniu oznacza „system nazw domen" (przyp. autora).

[36] M. Zelek, *Umowa o rejestrację domeny internetowej*, C.H. Beck, Warszawa 2015, s. 8.

ulec przekształceniu w formę bardziej globalną, ponieważ Internet spełnia ważną funkcję wspierania społeczeństwa i gospodarki na całym świecie[37].

O prawach autorskich i naruszeniach znaku towarowego w kontekście zagrożeń bezpieczeństwa cybernetycznego powinno się mówić nie tylko z powodu utraconych zysków w prowadzonej przez tę czy inną firmę działalności gospodarczej. Głównym powodem jest to, że transakcje zbycia podrobionych produktów bądź czynności polegające na łamaniu praw autorskich, określane jako piractwo internetowe, odbywają się w cyberprzestrzeni. W pierwszym wypadku istotnymi stają się odpowiednie regulacje w zakresie rejestracji nazw domen drugiego i dalszego poziomów, ażeby nie dochodziło nie tyle nawet do sporów związanych z posługiwaniem się nazwami zawierającymi zarejestrowany na rzecz innego podmiotu znak towarowy, ile do ich niewłaściwego, mylącego wykorzystywania (czyli nie tylko w sposób stanowiący czyn nieuczciwej konkurencji, na co wskazuje M. Zelek[38]). W wypadku piractwa internetowego, jak podkreśla A.A. Janowska[39], rolą polityki publicznej potencjalnie powinna być interwencja eliminująca zawodność rynku powodowaną przez dostępność w Internecie tzw. pirackich kopii, czyli utworów udostępnianych w sieci bez autoryzacji ze strony twórców.

Warto jednakże podkreślić, że na poziomie Unii Europejskiej od dłuższego czasu analizowano korzyści wynikające z rozwoju społeczeństwa informacyjnego, wskutek czego już w 2010 r. w dokumencie pt. *Europejska agenda cyfrowa*[40] określono wiele działań w dziedzinie praw autorskich, mających na celu otwarcie dostępu do treści w ramach strategii na rzecz osiągnięcia dynamicznego jednolitego rynku cyfrowego, co znalazło kontynuację w kolejnych dokumentach, w tym m.in. w *Strategii jednolitego rynku cyfrowego dla Europy*[41].

Ubocznym aspektem prowadzenia korespondencji w Internecie, wymagającej posiadania w serwisach pocztowych skrzynek e-mailowych, jest zjawisko określane mianem *spamming*. Polega ono na rozsyłaniu ich posiadaczom w postaci wiadomości e-mail niezamówionej informacji handlowej, czyli tzw. spamu. Etymologicznie

[37] Zob. Komunikat Komisji do Parlamentu Europejskiego, Rady, Europejskiego Komitetu Ekonomiczno-Społecznego i Komitetu Regionów, *Polityka wobec Internetu i zarządzanie Internetem: Rola Europy*…, op.cit., s. 6.

[38] M. Zelek, op.cit., s. 7.

[39] A.A. Janowska, *Polityka publiczna w zakresie otwartych zasobów: Unia Europejska*, Kwartalnik Kolegium Ekonomiczno-Społecznego SGH „Studia z Polityki Publicznej" 2014, nr 4(4), s. 117.

[40] Zob. Komunikat Komisji do Parlamentu Europejskiego, Rady, Europejskiego Komitetu Ekonomiczno-Społecznego i Komitetu Regionów, *Europejska agenda cyfrowa* (COM (2010) 245 final z 16.5.2010).

[41] Zob. Komunikat Komisji do Parlamentu Europejskiego, Rady, Europejskiego Komitetu Ekonomiczno-Społecznego i Komitetu Regionów, *Strategia jednolitego rynku cyfrowego dla Europy* (SWD (2015) 100 final z 6.5.2015).

pojęcie to, jak odnotowuje M. Czyżak[42], pochodzi z języka angielskiego i jest skrótem wyrażenia *spiced pork and ham*, oznaczającego mielonkę i wskazującego na zawartość oraz charakter takiej informacji. Inną kategorią niechcianych wiadomości e-mailowych i komunikatów w sieciach socjalnych oraz, zarazem, postacią czynności bardziej szkodliwych aniżeli *spamming*, jest *phishing*, określany jako podstępne działanie polegające na pozyskiwaniu poufnych danych osobistych – takich, jak hasła internetowe i informacje dotyczące kart płatniczych, dzięki podszywaniu się pod instytucję albo osobę godną zaufania, która wyraża potrzebę niezwłocznego uzyskania tych informacji.

Nazwa tej metody popełniania przestępstw komputerowych bardzo często tłumaczona jest jako *password harvesting fishing*, czyli „łowienie haseł". Jednak niekiedy uważa się, iż ma z nią wiele wspólnego wykradanie numerów kart kredytowych poprzez socjotechnikę (jednym z jej pionierów był B. Phish)[43].

Komisja Europejska wykazała zainteresowanie kwestią rozsyłania niechcianej korespondencji e-mailowej w postaciach *spamming* i *phishing* jeszcze w listopadzie 2006 r., wystosowując do Rady Unii Europejskiej, Parlamentu Europejskiego, Europejskiego Komitetu Ekonomiczno-Społecznego oraz Komitetu Regionów komunikat poświęcony zwalczaniu spamu, oprogramowania szpiegowskiego i złośliwego oprogramowania[44].

Jak już wspomniano, w katalogu zagadnień, które powinny być regulowane przez politykę w zakresie cyberbezpieczeństwa, są zagadnienia związane z użytkownikami cyberprzestrzeni, w związku z czym z jednej strony warto poświęcić uwagę takim pojęciom, jak rozsyłanie złośliwego oprogramowania poprzez reklamę internetową (*malvertising*), podawanie się za kogoś innego (*impersonation*), odpowiednie korzystanie, cyberprzestępczość, geolokalizacja i prywatność, zaś z drugiej – postarać się przeanalizować, czy znajdują się one w kręgu zainteresowania polityki publicznej na forum Unii Europejskiej.

Termin *malvertising* jest wykorzystywany do określenia nowego zagrożenia, polegającego na rozpowszechnianiu złośliwej reklamy; nazwa powstała wskutek połączenia dwóch angielskich słów: *malvare* (złośliwe programy) i *advertising* (reklama)[45].

---

[42] M. Czyżak, *Spamming i jego karalność w polskim systemie prawnym*, „Pomiary – Automatyka – Kontrola" 2009, nr 7(55), s. 548.

[43] K. Karwowska, A. Folga, *Phishing: modus operandi sprawców oraz środki zapobiegawcze*, „Kortowski Przegląd Prawniczy. Czasopismo naukowe Wydziału Prawa i Administracji Uniwersytetu Warmińsko-Mazurskiego w Olsztynie" 2013, nr 4, s. 7.

[44] Zob. Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, *On Fighting Spam, Spyware and Malicious Software* (COM (2006) 688 final from 15.11.2006).

[45] Działanie *malvertising* polega na umieszczaniu złośliwego kodu lub skryptu w reklamach internetowych, który aktywowany jest po kliknięciu w reklamę.

Podawanie się za kogoś innego polega na manipulowaniu danymi w ramach sesji uwierzytelniania lub dokonywania zlecenia, dzięki zastosowaniu tej metody oszust jest uznawany przez system za jakiegoś konkretnego autoryzowanego użytkownika; metoda ta jest szeroko praktykowana przez różnego rodzaju internetowych oszustów, czynności wykonywane przez nich mogą polegać zarówno na rozsyłaniu tzw. postów w celu ich publikacji na forach internetowych, jak i na kradzieży danych z konta[46]. Mówiąc o cyberprzestępczości, należy we właściwy sposób odgraniczać od niej odpowiednie korzystanie z Internetu i cyberprzestrzeni, czyli mieszczące się w ramach obowiązującego prawa.

W polityce publicznej Unii Europejskiej problematyka ta od dłuższego czasu znajduje się w centrum uwagi. Wystarczy przywołać Komunikat Komisji do Parlamentu Europejskiego, Rady oraz Komitetu Regionów – *W kierunku ogólnej strategii zwalczania cyberprzestępczości*[47] oraz program sztokholmski – *Otwarta i bezpieczna Europa dla dobra i ochrony obywateli*[48] wraz z planem działania[49] służącym jego realizacji. Biorąc pod uwagę, iż geolokalizacji adresów IP nie można łączyć z faktycznym miejscem, z którego przeprowadzono atak cybernetyczny, gdyż dla ukrycia swojej tożsamości atakujący mogli używać serwerów pośredniczących (*proxy*) lub komputerów, nad którymi wcześniej przejęto kontrolę, na co wskazują np. M. Grzelak i K. Liedel[50], stwierdzić należy powstanie dylematu dotyczącego z jednej strony prywatności w sieci Internet, zaś z drugiej – skutecznego zwalczania cyberprzestępczości.

Warto odnotować, że jedną z zasad bezpieczeństwa cybernetycznego, deklarowanych przez Komisję Europejską[51], jest ochrona praw podstawowych, wolności wypowiedzi, danych osobowych i prywatności, przy czym podkreśla się, iż zapewnienie cyberbezpieczeństwa będzie zadowalające i skuteczne tylko wtedy, kiedy będzie ono oparte na podstawowych prawach i swobodach zapisanych w Karcie praw podstawowych Unii Europejskiej oraz na podstawowych wartościach UE. Wszelka wymiana informacji do celów zapewnienia bezpieczeństwa cybernetycznego w sytuacji, gdy

[46] Por. J.L. Bayuk, J. Healey, P. Rohmeyer, M.H. Sachs, J. Schmidt, J. Weiss, *Cyber Security*…, op.cit., s. 115, 247.

[47] Zob. Komunikat Komisji do Parlamentu Europejskiego, Rady oraz Komitetu Regionów, *W kierunku ogólnej strategii zwalczania cyberprzestępczości* (KOM (2007) 267 wersja ostateczna z 22.5.2007).

[48] Zob. program sztokholmski – *Otwarta i bezpieczna Europa dla dobra i ochrony obywateli*, Dz. Urz. UE 2010 C 115.

[49] Zob. *Komunikat Komisji* do Parlamentu Europejskiego, Rady, Europejskiego Komitetu Ekonomiczno-Społecznego oraz Komitetu Regionów, *Przestrzeń wolności, bezpieczeństwa i sprawiedliwości dla europejskich obywateli – Plan działań służący realizacji programu sztokholmskiego* (KOM (2010) 171 wersja ostateczna z 20.4.2010).

[50] M. Grzelak, K. Liedel, *Bezpieczeństwo w cyberprzestrzeni. Zagrożenia i wyzwania dla Polski – zarys problemu*, „Bezpieczeństwo Narodowe" 2012, nr 22 (II), s. 135–136.

[51] Zob. Wspólny komunikat Komisji do Parlamentu Europejskiego, Rady, Europejskiego Komitetu Ekonomiczno-Społecznego i Komitetu Regionów, *Strategia bezpieczeństwa cybernetycznego*…, op.cit., s. 4.

w grę wchodzą dane osobowe, powinna być zatem zgodna z unijnymi przepisami dotyczącymi ochrony danych i powinna w pełni uwzględniać prawa obywateli w tej dziedzinie.

Warto równocześnie odnieść się do Komunikatu Komisji Europejskiej dotyczącego realizacji założeń programu sztokholmskiego[52]. W dokumencie tym w rozdziale zatytułowanym *Europa, która chroni* poświęcono uwagę podniesieniu poziomu ochrony obywateli i przedsiębiorstw w cyberprzestrzeni poprzez:

- zwiększenie zdolności operacyjnej zwalczania cyberprzestępczości (Unia Europejska utworzyła Europejskie Centrum ds. Walki z Cyberprzestępczością – EC3 przy biurze Europolu, w związku z czym, o ile to możliwe, zaleca utworzenie centrów ds. walki z cyberprzestępczością we wszystkich państwach członkowskich),
- kontynuację współpracy ze Stanami Zjednoczonymi w ramach wspólnie utworzonego światowego sojuszu przeciwko niegodziwemu traktowaniu dzieci w Internecie w celach seksualnych,
- wdrożenie uzgodnionych przez Unię Europejską zaostrzonych przepisów mających na celu zwalczanie cyberprzestępczości,
- zacieśnienie współpracy z sektorem prywatnym,
- ustalenie jurysdykcji w cyberprzestrzeni, m.in. dzięki ratyfikowaniu konwencji Rady Europy o cyberprzestępczości przez państwa, które jeszcze tego nie zrobiły.

Odnosząc się do kolejnych zagadnień, które powinny być regulowane przez politykę w zakresie cyberbezpieczeństwa, wymieniono zagadnienia związane z cyberkonfliktami.

Pozornie wydawać się może, że problematyka ścigania sprawców kradzieży własności intelektualnej w Internecie znajduje się obecnie poza kręgiem zainteresowania Unii Europejskiej, co pośrednio potwierdza np. przyjęta w 2011 r. strategia pt. *Jednolity rynek w obszarze praw własności intelektualnej*[53], w której brak jest odpowiednich zapisów. W lipcu 2012 r. Parlament Europejski odrzucił koncepcję regulacji Internetu[54], zaproponowaną zapisami umowy handlowej dotyczącej zwalczania obrotu towarami podrabianymi (Anti-Counterfeiting Trade Agreement

[52] Zob. Komunikat Komisji do Parlamentu Europejskiego, Rady, Europejskiego Komitetu Ekonomiczno-Społecznego oraz Komitetu Regionów, *Otwarta i bezpieczna Europa: realizacja założeń* (COM (2014) 154 final z 11.3.2014).

[53] Zob. Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, *A Single Market for Intellectual Property Rights: Boosting Creativity and Innovation to Provide Economic Growth, High Quality Jobs and First Class Products and Services in Europe* (COM (2011) 287 final from 24.5.2011).

[54] Por. T. Niedziółka, *Regulacja Internetu a rozwój Unii Europejskiej*, Biuletyn „Opinie Fundacji Amicus Europae" 2012, nr 16, s. 2.

– ACTA), która miała ustalić międzynarodowe standardy w walce z naruszeniami własności intelektualnej[55].

Obecnie jednak Unia Europejska negocjuje ze Stanami Zjednoczonymi umowę o Transatlantyckim Partnerstwie Handlowo-Inwestycyjnym (Transatlantic Trade and Investment Partnership – TTIP), która ma stworzyć nowe, wymagające i dostosowane do wyzwań współczesności reguły współpracy w wielu obszarach mających duży wpływ na wymianę handlową, np. w obszarze prawa własności intelektualnej[56]. Jak odnotowuje A. Pietraszewska[57], z pojedynczych informacji, udzielanych m.in. przez Komisję Europejską prowadzącą negocjacje, można wywnioskować, że TTIP w wielu aspektach przypomina ACTA i jest próbą wprowadzenia tych rozwiązań, które w poprzedniej umowie nie zostały zaakceptowane. W innych źródłach[58] stwierdza się jednak, iż mitem jest to, że TTIP będzie „drugą umową ACTA" i wprowadzi sankcje karne w środowisku cyfrowym.

Nawiązując do cyberszpiegostwa i cybersabotażu, rozpatrywanych w kontekście zagadnień, które powinny znaleźć się w kręgu zainteresowania polityki publicznej w zakresie cyberbezpieczeństwa, należy odnotować, iż w dokumencie roboczym Komisji Europejskiej pt. *Przegląd przyrodniczych i antropogenicznych zagrożeń w UE*[59] klasyfikują się one jako przykłady syntaktycznych cyberataków, a więc takich, podczas których wykorzystuje się złośliwe oprogramowanie (np. wirusy, robaki, konie trojańskie) – w przeciwieństwie do ataków semantycznych, realizowanych za pośrednictwem rozpowszechniania nieprawdziwych informacji.

W Unii Europejskiej istnieją dwa główne obszary polityki w zakresie bezpieczeństwa cyberprzestrzeni, które mają znaczenie z punktu widzenia cybernetycznych działań wojennych (*cyber warfare*). Do pierwszego należą regulacje ukierunkowane na zwalczanie cyberataków (w tym również cyberprzestępczości i cyberterroryzmu), do drugiego – mające na celu ochronę infrastruktury krytycznej (Critical Infrastructure Protection – CIP), krytycznej infrastruktury informatycznej (Critical Information Infrastructure

[55] Szerzej: Wniosek. Decyzja Rady w sprawie zawarcia umowy handlowej dotyczącej zwalczania obrotu towarami podrobionymi między Unią Europejską i jej Państwami Członkowskimi, Australią, Kanadą, Japonią, Republiką Korei, Meksykańskimi Stanami Zjednoczonymi, Królestwem Marokańskim, Nową Zelandią, Republiką Singapuru, Konfederacją Szwajcarską i Stanami Zjednoczonymi Ameryki (KOM (2011) 380 wersja ostateczna z 24.6.2011); umowa ta budziła spore kontrowersje.

[56] Por. W. Gadomski, T. Kalinowski, M. Rot, E. Sadowska-Cieślak, *Fakty i mity o TTIP: Negocjacje umowy o wolnym handlu pomiędzy Stanami Zjednoczonymi a Unią Europejską (Transatlantyckie Partnerstwo Handlowo-Inwestycyjne)*, Ministerstwo Spraw Zagranicznych, Warszawa 2015, s. 5, 18.

[57] A. Pietraszewska, *Czy jest się czego obawiać, czyli o ingerencji umów ACTA i TTIP w ochronę prawa autorskiego w Sieci*, Zeszyt naukowy Naukowego Koła Cywilistów Uniwersytetu Wrocławskiego „Prawa Autorskie i Własność Przemysłowa" 2015, s. 84.

[58] W. Gadomski, T. Kalinowski, M. Rot, E. Sadowska-Cieślak, op.cit., s. 40.

[59] Zob. Commission Staff Working Document, *Overview of Natural and Man-made Disaster Risks in the EU* (SWD (2014) 134 final from 8.4.2014), s. 43.

Protection, CIIP) oraz bezpieczeństwa sieci i informacji (Network and Information Security, NIS)[60]. Wszelkie działania w zakresie pierwszego obszaru, na co wskazuje A. Kańciak[61], podlegają przepisom Tytułu V (*Przestrzeń wolności, bezpieczeństwa i sprawiedliwości*) Traktatu o funkcjonowaniu Unii Europejskiej (TFUE)[62]. Dlatego też, zgodnie z przedmiotowym i kompetencyjnym podziałem struktur unijnych, problematyka ta jest podejmowana przez Dyrekcję Generalną do Spraw Wewnętrznych i Migracji (Directorate General for Migration and Home Affairs). Z kolei drugi obszar znajduje się w kompetencji Dyrekcji Generalnej ds. Sieci komunikacyjnych, treści i technologii (Directorate General for Communications Networks, Content and Technology) i jest uregulowany w Tytule VIII (*Polityka gospodarcza i pieniężna*) TFUE[63]. Kamień milowy w pierwszym z obszarów stanowiła Decyzja ramowa Rady 2005/222/WSiSW z dnia 24 lutego 2005 r. w sprawie ataków na systemy informatyczne[64], zastąpiona Dyrektywą Parlamentu Europejskiego i Rady 2013/40/UE z dnia 12 sierpnia 2013 r. dotyczącą ataków na systemy informatyczne i uchylającą decyzję ramową Rady 2005/222/WSiSW[65]. Przybliżając regulacje dotyczące drugiego obszaru, należy nadmienić, iż jeszcze w 2001 r. Komisja Europejska opracowała politykę dotyczącą bezpieczeństwa sieci i informacji (Network and Information Security, NIS). Pod koniec 2005 r. Komisja Europejska opracowała Zieloną księgę w sprawie europejskiego programu ochrony infrastruktury krytycznej[66], w załączniku nr 1 do której zawarto definicje obu typów infrastruktur krytycznych. Ochronę infrastruktury krytycznej objęto odrębną regulacją Unii Europejskiej – Dyrektywą Rady 2008/114/WE z dnia 8 grudnia 2008 r. w sprawie rozpoznawania i wyznaczania europejskiej infrastruktury krytycznej oraz oceny potrzeb w zakresie poprawy jej ochrony[67], będącą podstawowym elementem Europejskiego Programu Ochrony Infrastruktury Krytycznej (EPOIK).

---

[60] *Cybersecurity and Cyberpower: Concepts, Conditions and Capabilities for Cooperation for Action within the EU*, European Parliament, Directorate-General for External policies of the Union, EXPO/B/SEDE/FWC/2009–01/LOT6/09, April 2011, s. 36.

[61] A. Kańciak, *Problematyka cyberprzestępczości w Unii Europejskiej*, „Przegląd Bezpieczeństwa Wewnętrznego" 2013, nr 8, s. 112.

[62] Zob. Wersja skonsolidowana Traktatu o funkcjonowaniu Unii Europejskiej (TFUE), Dz. Urz. UE C 326/47 z 26.10.2012, z późn. zm., s. 73–85.

[63] Ibidem, s. 96–112.

[64] Zob. Decyzja ramowa Rady 2005/222/WSiSW z dnia 24 lutego 2005 r. w sprawie ataków na systemy informatyczne, Dz. Urz. UE L 69 z 16.03.2005.

[65] Zob. Dyrektywa Parlamentu Europejskiego i Rady 2013/40/UE z dnia 12 sierpnia 2013 r. dotycząca ataków na systemy informatyczne i uchylająca decyzję ramową Rady 2005/222/WSiSW, Dz. Urz. UE L 218 z 14.08.2013.

[66] Zob. *Zielona księga w sprawie europejskiego programu ochrony infrastruktury krytycznej*, Komisja Wspólnot Europejskich (KOM (2005) 576 wersja ostateczna z 17.11.2005).

[67] Zob. Dyrektywa Rady 2008/114/WE z dnia 8 grudnia 2008 r. w sprawie rozpoznawania i wyznaczania europejskiej infrastruktury krytycznej oraz oceny potrzeb w zakresie poprawy jej ochrony, Dz. Urz. UE L 345 z 23.12.2008.

Krytycznej infrastrukturze informatycznej poświęcono dwa komunikaty Komisji do Parlamentu Europejskiego, Rady, Europejskiego Komitetu Ekonomiczno-Społecznego i Komitetu Regionów, z 2009 i 2011 r. W pierwszym z nich pt. *Ochrona Europy przed zakrojonymi na szeroką skalę atakami i zakłóceniami cybernetycznymi: zwiększenie gotowości, bezpieczeństwa i odporności*[68] stwierdza się, że niektóre systemy, usługi, sieci i infrastrukturę ICT uważa się zwykle za krytyczną infrastrukturę informatyczną, ponieważ zakłócenie ich działalności lub zniszczenie miałoby poważne konsekwencje dla kluczowych aspektów funkcjonowania społeczeństwa.

Równocześnie określono plan działania (*The CIIP Action Plan*) oparty na pięciu filarach: gotowości i zapobieganiu, wykrywaniu i reagowaniu, łagodzeniu skutków i przywracaniu sprawności operacyjnej, współpracy międzynarodowej i kryteriach rozpoznawania europejskich infrastruktur krytycznych w sektorze ICT[69]. Weryfikacji jego wykonywania poświęcono komunikat pt. *Osiągnięcia i kolejne etapy: w kierunku globalnego cyberbezpieczeństwa*[70]. W ostatnich latach na forum Unii Europejskiej podejmowane są inicjatywy na rzecz dostosowania regulacji z dziedziny cyberbezpieczeństwa do nowej rzeczywistości. W wielu państwach członkowskich i na poziomie Unii Europejskiej brakowało do tej pory rozwiązań prawnych i instytucjonalnych w tej dziedzinie. Zmieni to przyjęcie dokumentu znanego jako NIS Directive (Network and Information Security Directive), czyli Dyrektywy o bezpieczeństwie sieci i informacji. NIS Directive ma skupiać się na ochronie infrastruktury krytycznej państw członkowskich[71].

Odnosząc się do szczegółowych problemów zarządzania cyberprzestrzenią, warto nadmienić, iż część z nich znajduje się poza kręgiem zainteresowania unijnej polityki publicznej w zakresie ochrony cyberprzestrzeni, zaś kluczowe znaczenie z tego punktu widzenia ma *Strategia bezpieczeństwa cybernetycznego Unii Europejskiej*. W dokumencie tym sformułowano zasady bezpieczeństwa cybernetycznego oraz poświęcono należytą uwagę problematyce badań i rozwoju, wskazując, że powinny one zapewnić przygotowanie do walki z nowymi problemami, jakie mogą się pojawić, zaś Unia Europejska powinna optymalnie wykorzystać program ramowy w zakresie

[68] Zob. Komunikat Komisji do Parlamentu Europejskiego, Rady, Europejskiego Komitetu Ekonomiczno-Społecznego oraz Komitetu Regionów w sprawie ochrony krytycznej infrastruktury informatycznej *Ochrona Europy przed zakrojonymi na szeroką skalę atakami i zakłóceniami cybernetycznymi: zwiększenie gotowości, bezpieczeństwa i odporności* (KOM (2009) 149 wersja ostateczna z 30.3.2009), s. 2.

[69] Ibidem, s. 9–13.

[70] Zob. Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, *On Critical Information Infrastructure Protection „Achievements and Next Steps: Towards Global Cyber-security* (COM (2011) 163 final from 31.3.2011).

[71] *Cyberbezpieczeństwo – problem nas wszystkich? Strategie państw UE wobec wyzwań związanych z dostępem do danych w sieci*, „Raporty i Analizy Centrum Stosunków Międzynarodowych" 2015, nr 1(5), s. 2.

badań naukowych i innowacji *Horyzont 2020*[72]. Ponieważ zagadnienia związane z zarządzaniem ryzykiem przedstawiono wcześniej, pozostaje omówić istniejące w Unii Europejskiej regulacje dotyczące bezpieczeństwa danych osobowych. W dniu 12 marca 2014 r. Parlament Europejski przyjął pakiet bardzo istotnych rezolucji:

- Rezolucję Parlamentu Europejskiego z dnia 12 marca 2014 r. w sprawie realizowanych przez NSA amerykańskich programów nadzoru, organów nadzoru w różnych państwach członkowskich oraz ich wpływu na prawa podstawowe obywateli UE oraz na współpracę transatlantycką w dziedzinie wymiaru sprawiedliwości i spraw wewnętrznych[73], dotyczącą inwigilacji obywateli Unii Europejskiej przez służby specjalne ze Stanów Zjednoczonych,
- Rezolucję ustawodawczą Parlamentu Europejskiego z dnia 12 marca 2014 r. w sprawie wniosku dotyczącego rozporządzenia Parlamentu Europejskiego i Rady w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i swobodnym przepływem takich danych (ogólne rozporządzenie o ochronie danych)[74],
- Rezolucję ustawodawczą Parlamentu Europejskiego z dnia 12 marca 2014 r. w sprawie wniosku dotyczącego dyrektywy Parlamentu Europejskiego i Rady w sprawie ochrony osób fizycznych w zakresie przetwarzania danych osobowych przez właściwe organy do celów zapobiegania przestępstwom, prowadzenia dochodzeń w ich sprawie, wykrywania ich i ścigania albo wykonywania kar kryminalnych oraz swobodnego przepływu tych danych[75].

Następnie, w grudniu 2015 r., Komisja Europejska opublikowała komunikat prasowy pt. *Porozumienie w sprawie reformy ochrony danych w UE ożywi jednolity rynek cyfrowy*[76], z którego wynika, iż reforma spowoduje, że w całej Unii Europejskiej będą

[72] Program ten ma wspierać badania w dziedzinie bezpieczeństwa związane z nowymi technologiami ICT, dostarczać rozwiązania dla bezpiecznych systemów, usług i aplikacji ICT typu *end-to-end*, zapewniać odpowiednie zachęty do wdrażania i przyjmowania istniejących rozwiązań oraz uwzględniać kwestię interoperacyjności sieci i systemów informatycznych.

[73] Zob. Rezolucja Parlamentu Europejskiego z dnia 12 marca 2014 r. w sprawie realizowanych przez NSA amerykańskich programów nadzoru, organów nadzoru w różnych państwach członkowskich oraz ich wpływu na prawa podstawowe obywateli UE oraz na współpracę transatlantycką w dziedzinie wymiaru sprawiedliwości i spraw wewnętrznych, 2013/2188 (INI).

[74] Zob. Rezolucja ustawodawcza Parlamentu Europejskiego z dnia 12 marca 2014 r. w sprawie wniosku dotyczącego rozporządzenia Parlamentu Europejskiego i Rady w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i swobodnym przepływem takich danych (ogólne rozporządzenie o ochronie danych), COM (2012) 0011–2012/0011 (COD).

[75] Zob. Rezolucja ustawodawcza Parlamentu Europejskiego z dnia 12 marca 2014 r. w sprawie wniosku dotyczącego dyrektywy Parlamentu Europejskiego i Rady w sprawie ochrony osób fizycznych w zakresie przetwarzania danych osobowych przez właściwe organy do celów zapobiegania przestępstwom, prowadzenia dochodzeń w ich sprawie, wykrywania ich i ścigania albo wykonywania kar kryminalnych oraz swobodnego przepływu tych danych, COM (2012) 0010.

[76] Zob. *Porozumienie w sprawie reformy ochrony danych w UE ożywi jednolity rynek cyfrowy*, Komunikat prasowy Komisji Europejskiej, Bruksela, 15 grudnia 2015.

obowiązywały jednakowe przepisy, zaś w dniu 29 lutego 2016 r. pojawił się Komunikat Komisji do Parlamentu Europejskiego i Rady pt. *Transatlantyckie przepływy danych: odbudowa zaufania dzięki ustanowieniu silniejszych gwarancji*[77].

Strategie państw członkowskich Unii Europejskiej w zakresie cyberbezpieczeństwa

Cyberprzestrzeń oferuje duże możliwości wzrostu gospodarczego i rozwoju społecznego, jednakże zagrożenia płynące z niej wymagają skoordynowanych działań w celu zapewnienia jej ochrony. Ustanawiając w 2004 r. na mocy Rozporządzenia Parlamentu Europejskiego i Rady (WE) nr 460/2004[78] Europejską Agencję ds. Bezpieczeństwa Sieci i Informacji (ENISA), wychodzono z założenia, iż instytucja ta nie tylko przyczyni się do realizacji celów w zakresie zapewnienia wysokiego poziomu bezpieczeństwa sieci i informacji w Unii Europejskiej, lecz także będzie sprzyjała swoją działalnością rozwijaniu kultury bezpieczeństwa sieci i informacji na rzecz obywateli, konsumentów, przedsiębiorstw oraz administracji publicznej.

W 2008 r. Parlament Europejski i Rada przyjęły Rozporządzenie (WE) nr 1007/2008[79] przedłużające mandat Agencji do marca 2012 r., natomiast Rozporządzenie (WE) nr 580/2011[80] przedłużyło mandat Agencji do dnia 13 września 2013 r., po czym – w odpowiedzi na zmieniające się wyzwania – na mocy Rozporządzenia Parlamentu Europejskiego i Rady (UE) nr 526/2013 z dnia 21 maja 2013 r.[81] powołano następcę ENISA ustanowionej w 2004 r. W myśl regulacji zawartych w przywołanym rozporządzeniu[82] Agencji tej powinny być przekazywane strategie na rzecz bezpieczeństwa sieci i informacji ogłaszane przez instytucje, organy, urzędy lub agencje Unii Europejskiej albo przez państwa członkowskie w celach informacyjnych oraz aby unikać powielania pracy. Agencja powinna dokonywać

[77] Zob. Komunikat Komisji do Parlamentu Europejskiego, Rady, *Transatlantyckie przepływy danych: odbudowa zaufania dzięki ustanowieniu silniejszych gwarancji* (COM (2016) 117 final z 29.2.2016).

[78] Zob. Rozporządzenie Parlamentu Europejskiego i Rady (WE) nr 460/2004 z dnia 10 marca 2004 r. ustanawiające Europejską Agencję ds. Bezpieczeństwa Sieci i Informacji, Dz. Urz. UE L 77 z 13.03.2004.

[79] Zob. Rozporządzenie Parlamentu Europejskiego i Rady (WE) nr 1007/2008 z dnia 24 września 2008 r. zmieniające rozporządzenie (WE) nr 460/2004 ustanawiające Europejską Agencję ds. Bezpieczeństwa Sieci i Informacji w zakresie okresu jej działania, Dz. Urz. UE L 293 z 31.10.2008.

[80] Zob. Rozporządzenie Parlamentu Europejskiego i Rady (UE) nr 580/2011 z dnia 8 czerwca 2011 r. zmieniające rozporządzenie (WE) nr 460/2004 ustanawiające Europejską Agencję ds. Bezpieczeństwa Sieci i Informacji w zakresie okresu jej działania, Dz. Urz. UE L 165 z 24.6.2011.

[81] Zob. Rozporządzenie Parlamentu Europejskiego i Rady (UE) nr 526/2013 z dnia 21 maja 2013 r. w sprawie Agencji Unii Europejskiej ds. Bezpieczeństwa Sieci i Informacji (ENISA) oraz uchylające rozporządzenie (WE) nr 460/2004, Dz. Urz. UE L 165 z 18.6.2013.

[82] Ibidem, s. 43.

analizy tych strategii oraz publicznie udostępniać strategie i ich analizy za pomocą środków elektronicznych.

W listopadzie 2014 r. ENISA opracowała ramy oceny narodowych strategii cyberbezpieczeństwa[83], koncentrując się na aspekcie oceny ich cyklu życia i mając na uwadze realizację czterech celów, a mianowicie:

- przeprowadzenie krytycznej analizy stosowanego podejścia do oceny narodowych strategii cyberbezpieczeństwa,
- przedstawienie zaleceń i identyfikację dobrych praktyk w zakresie wdrażania tych strategii i ich oceny,
- zaprojektowanie i opracowanie zasad oceny,
- utworzenie zestawu kluczowych wskaźników efektywności zastosowanego rozwiązania, aby mieć możliwość dostosowywania ramowych regulacji w zakresie oceny strategii do zmieniających się potrzeb państw członkowskich na różnych poziomach zaawansowania w planowaniu strategicznym[84].

W 2015 r. BSA – The Software Alliance, światowa organizacja z siedzibą w Waszyngtonie, reprezentująca interesy firm z branży oprogramowania i angażująca się w kształtowanie polityki publicznej promującej innowacyjne technologie oraz pobudzanie wzrostu gospodarczego, dokonała analizy przepisów, regulacji i zasad dotyczących cyberbezpieczeństwa w 28 państwach członkowskich Unii Europejskiej.

Przygotowanie tych państw do zapewnienia bezpieczeństwa w cyberprzestrzeni analizowano według 25 kryteriów zgrupowanych wokół pięciu tematów – podstaw prawnych funkcjonowania cyberbezpieczeństwa, jednostek organizacyjnych, partnerstwa publiczno-prywatnego, sektorowego cyberbezpieczeństwa oraz edukacji.

Korzystając z danych przedstawionych w raporcie sporządzonym w wyniku przeprowadzonego przez BSA – The Software Alliance badania[85], można stwierdzić, iż według stanu na 3 marca 2015 r. (data opublikowania raportu), narodowe strategie cyberbezpieczeństwa były przyjęte przez 19 z 28 państw, przy czym spośród ośmiu, w których nie zdążono przyjąć strategii, jedynie w Portugalii odpowiednia strategia znajdowała się w stadium opracowywania.

Narodowej strategii cyberbezpieczeństwa nie mają takie państwa, jak (kolejność alfabetyczna): Bułgaria, Chorwacja, Dania, Grecja, Irlandia, Malta, Słowenia i Szwecja. Najpóźniej – w 2014 r. – przyjęto ją w Estonii, na Łotwie i we Włoszech, najwcześniej – w 2008 r. – w Słowacji. Nie we wszystkich państwach członkowskich

[83] *An Evaluation Framework for National Cyber Security Strategies*, European Union Agency for Network and Information Security, Heraklion 2014.

[84] Ibidem, s. 3.

[85] *EU Cybersecurity Dashboard – A Path to Secure European Cyberspace*, BSA – The Software Alliance, Washington 2015.

Unii Europejskiej opracowano i przyjęto plan bądź strategię ochrony infrastruktury krytycznej, brakuje takiego dokumentu w ośmiu państwach, natomiast w pięciu zostało zastosowane rozwiązanie uznane za realizatorów badania za połowiczne.

Opierając się na przedstawionych kryteriach, można zbudować ranking państw członkowskich Unii Europejskich uwzględniający ich przygotowanie do zapewnienia cyberbezpieczeństwa. W tym celu wystarczy przypisać[86]:

- występowaniu pożądanej cechy znaczenie – 1,
- częściowemu występowaniu pożądanej cechy – 0,5,
- niewystępowaniu pożądanej cechy lub stwierdzeniu „nie dotyczy" – 0.

Datom przyjęcia narodowej strategii cyberbezpieczeństwa oraz powołania CERT przypisano następujące wartości:

- przyjęcie strategii w/lub po roku 2014 czy powołanie CERT w/lub po roku 2013–1,
- przyjęcie strategii przed rokiem 2014 lub powołanie CERT przed rokiem 2013–0,5,
- brak strategii i/lub brak CERT – 0.

Zastosowaną metodę ilustruje tabela 1.

Tabela 1. Przypisanie znaczeń kryteriom oceny

Lp.	Nazwa kryterium	Występuje; strategia 2014, CERT 2013 (i później)	Nie występuje	Występuje częściowo; strategia przed 2014, CERT przed 2013
Zakres tematyczny: Podstawy prawne funkcjonowania cyberbezpieczeństwa				
1.	Istnienie narodowej strategii cyberbezpieczeństwa	1	0	0,5
2.	Rok przyjęcia narodowej strategii cyberbezpieczeństwa	1	0	0,5
3.	Istnienie planu lub strategii ochrony infrastruktury krytycznej	1	0	0,5
4.	Istnienie ustawowego lub wynikającego z przyjętej polityki wymogu ustanowienia pisemnego planu dotyczącego bezpieczeństwa informacyjnego	1	0	0,5
5.	Istnienie ustawowego lub wynikającego z przyjętej polityki wymogu dokonywania inwentaryzacji „systemu" i klasyfikacji danych	1	0	0,5
6.	Istnienie ustawowego lub wynikającego z przyjętej polityki wymogu odpowiedniego mapowania praktycznych rozwiązań lub wymagań w zakresie cyberbezpieczeństwa zgodnie z poziomem ryzyka	1	0	0,5
7.	Istnienie ustawowego lub wynikającego z przyjętej polityki wymogu przeprowadzania audytu stanu cyberbezpieczeństwa co najmniej jeden raz w skali rocznej	1	0	0,5
8.	Istnienie ustawowego lub wynikającego z przyjętej polityki wymogu dokonywania publicznego sprawozdania na temat stanu cyberbezpieczeństwa dla rządu	1	0	0,5

[86] Autorzy raportu nie uwzględniali możliwości występowania niepożądanych cech.

9.	Istnienie ustawowego lub wynikającego z przyjętej polityki wymogu posiadania w instytucjach państwowych stanowisk dyrektorów odpowiedzialnych za bezpieczeństwo lub informatykę (Chief Information Officer – CIO oraz Chief Security Officer – CSO)	1	0	0,5
10.	Istnienie ustawowego lub wynikającego z przyjętej polityki wymogu obligatoryjnego zgłaszania incydentów naruszenia cyberbezpieczeństwa	1	0	0,5
11.	Istnienie prawnej lub zawartej w przyjętej polityce definicji pojęcia „ochrona infrastruktury krytycznej”	1	0	0,5
12.	Istnienie wymagań dotyczących zamówień publiczno-prywatnych w zakresie rozwiązań z dziedziny cyberbezpieczeństwa opartych na międzynarodowych systemach akredytacji lub certyfikacji, bez dodatkowych wymagań lokalnych	1	0	0,5
Zakres tematyczny: Jednostki organizacyjne				
1.	Istnienie Zespołu Reagowania na Incydenty Komputerowe (Computer Emergency Response Team, CERT) lub Zespołu ds. Bezpieczeństwa Komputerowego i Reagowania na Incydenty (Computer Security and Incident Response Team, CSIRT)	1	0	0,5
2.	Rok powołania CERT	1	0	0,5
3.	Istnienie krajowego organu właściwego do spraw związanych z bezpieczeństwem informacji w Internecie (Network and Information Security, NIS)	1	0	0,5
4.	Istnienie platformy informatycznej pozwalającej raportować i gromadzić dane dotyczące incydentów naruszenia cyberbezpieczeństwa	1	0	0,5
5.	Przeprowadzanie ogólnokrajowych ćwiczeń w zakresie cyberbezpieczeństwa	1	0	0,5
6.	Istnienie krajowej struktury odpowiedzialnej za zarządzanie zdarzeniami (National Incident Management Structure, NIMS) dla reagowania na incydenty dotyczące naruszenia cyberbezpieczeństwa	1	0	0,5
Zakres tematyczny: Partnerstwo publiczno-prywatne				
1.	Istnienie rozwiązań dotyczących partnerstwa publiczno-prywatnego w zakresie cyberbezpieczeństwa	1	0	0,5
2.	Istnienie zorganizowanych struktur biznesowych odpowiedzialnych za cyberbezpieczeństwo	1	0	0,5
3.	Planowanie lub przygotowanie nowych inicjatyw publiczno-prywatnych w zakresie cyberbezpieczeństwa	1	0	0,5
Zakres tematyczny: Sektorowe plany cyberbezpieczeństwa				
1.	Istnienie wspólnego publiczno-prywatnego planu sektorowego dotyczącego cyberbezpieczeństwa	1	0	0,5
2.	Posiadanie przez sektor zdefiniowanych specyficznych obszarów, w których powinno być zapewnione cyberbezpieczeństwo	1	0	0,5
3.	Posiadanie przez ten czy ów sektor (branżę) ocen ryzyka dla cyberbezpieczeństwa	1	0	0,5
Zakres tematyczny: Edukacja				
1.	Istnienie strategii edukacji mającej na celu zwiększenie wiedzy i wzrostu świadomości młodego pokolenia w zakresie cyberbezpieczeństwa	1	0	0,5

Źródło: opracowanie własne.

Metodologicznie przyjęte kryteria oceny różnią się od kryteriów stosowanych przez ENISA, niemniej sprawiają wrażenie bardziej uszczegółowionych. Ranking państw przedstawia tabela 2.

Tabela 2. Ranking państw

Nazwa państwa	Miejsce	Liczba punktów
Austria, Estonia	1	18
Holandia, Wielka Brytania	2	17,5
Czechy, Finlandia	3	17
Niemcy, Włochy, Hiszpania	4	16,5
Węgry	5	16
Łotwa	6	15,5
Litwa	7	14
Rumunia	8	13,5
Polska, Szwecja	9	13
Belgia, Słowacja	10	12,5
Francja	11	12
Dania	12	10,5
Bułgaria, Słowenia	13	10
Luksemburg	14	9,5
Grecja	15	9
Malta, Portugalia	16	8,5
Chorwacja	17	7,5
Cypr	18	5
Irlandia	19	3

Źródło: opracowanie własne.

Czołowe pozycje w rankingu zajmują takie państwa, jak Austria, Estonia, Holandia, Wielka Brytania, Finlandia i Czechy. Estonia jako jedno z pierwszych państw przyjęła w 2008 r. strategię bezpieczeństwa cybernetycznego, zaktualizowaną w 2014 r. Państwo to ma dobrze rozwinięty zespół CERT, w 2008 r. w Tallinie utworzono Centrum Doskonalenia Obrony Cybernetycznej NATO, a zaktualizowana strategia bezpieczeństwa cybernetycznego na lata 2014–2017 uznaje za główny cel wzmocnienie cybernetycznej tarczy[87].

Na tle pozostałych państw członkowskich Unii Europejskiej Polska pod względem zapewnienia cyberbezpieczeństwa prezentuje się wystarczająco pozytywnie, jeżeli brać pod uwagę kryteria, które znajdują się u podstaw przedstawionego rankingu.

[87] *Cyberbezpieczeństwo – problem nas wszystkich? Strategie państw UE wobec wyzwań związanych z dostępem do danych w sieci*, „Raporty i Analizy Centrum Stosunków Międzynarodowych" 2015, nr 1(5), s. 4.

Równocześnie, jak odnotowują M. Adamczuk i K. Liedel[88], Polska dopiero rozpoczęła budowę zintegrowanego systemu bezpieczeństwa cyberprzestrzeni. Jednym z jego elementów jest przyjęcie przez Komitet Stały Rady Ministrów w dniu 25 czerwca 2013 r. dokumentu *Polityka ochrony cyberprzestrzeni Rzeczypospolitej Polskiej*. Według wspomnianych autorów, zawiera on spójną koncepcję systemu zarządzania cyberprzestrzenią, a także w racjonalny sposób definiuje zależności między poszczególnymi organami i instytucjami państwowymi oraz ich wyspecjalizowanymi komórkami odpowiedzialnymi za zapewnienie odpowiedniego poziomu bezpieczeństwa teleinformatycznego w cyberprzestrzeni, nie jest to jednak dokument o charakterze transsektorowym, a jedynie rządowy[89]. W syntetycznej ocenie przedstawionej w raporcie BSA[90] również podkreśla się, że Polska ma kompleksowo opracowaną strategię z jasno określonymi celami. Odnotowuje się w nim ponadto, iż ze względu na to, że została ona przyjęta dopiero w 2013 r., większość z zaleceń jest nadal wdrażana.

W Informacji Najwyższej Izby Kontroli o wynikach kontroli planowej nr P/14/043 – *Realizacja przez podmioty państwowe zadań w zakresie ochrony cyberprzestrzeni Rzeczypospolitej Polskiej*[91], której głównym celem było sprawdzenie, w jaki sposób administracja państwowa zarządza ryzykiem związanym z zagrożeniami występującymi w cyberprzestrzeni RP, stwierdza się natomiast, iż *Polityka ochrony cyberprzestrzeni Rzeczypospolitej Polskiej* jest dokumentem powstałym w wyniku źle rozumianego kompromisu, w związku z czym cechuje go nieprecyzyjność. Podkreśla się nawet, że jest on obarczony wieloma błędami merytorycznymi.

W wystąpieniu pokontrolnym[92] odnotowuje się, iż w dokumencie tym nie zawarto propozycji zmian legislacyjnych niezbędnych do stworzenia krajowego systemu ochrony cyberprzestrzeni RP, mimo wskazania, że podstawowym elementem realizacji założeń dokumentu *Polityka ochrony cyberprzestrzeni Rzeczypospolitej Polskiej* przewidzianym niezwłocznie do wykonania, są działania legislacyjne.

W 2015 r. *Polityka ochrony cyberprzestrzeni Rzeczypospolitej Polskiej* została uzupełniona przez *Doktrynę cyberbezpieczeństwa Rzeczypospolitej Polskiej*, zaś w 2016 r. Zespół zadaniowy Ministerstwa Cyfryzacji opracował *Założenia strategii cyberbezpieczeństwa*

---

[88] M. Adamczuk, K. Liedel, *Doktryna cyberbezpieczeństwa RP*, „Przegląd Bezpieczeństwa Wewnętrznego" 2015, nr 12, s. 282.

[89] Ibidem.

[90] *EU Cybersecurity Dashboard – A Path to Secure European Cyberspace*, BSA – The Software Alliance, Washington 2015, s. 15.

[91] Zob. *Realizacja przez podmioty państwowe zadań w zakresie ochrony cyberprzestrzeni RP*, Informacja o wynikach kontroli, KPB 4101–002–00/2014 – nr ewid. 42/2015/P/14/043/KPB, Departament Porządku i Bezpieczeństwa Wewnętrznego, Najwyższa Izba Kontroli, Warszawa 2015, s. 12.

[92] Zob. Wystąpienie pokontrolne Wiceprezesa Najwyższej Izby Kontroli W. Kutyły, KPB-4101–002–01/2014 P/14/043, Warszawa 2015, s. 12.

dla Rzeczypospolitej Polskiej[93]. Jak podkreśla się w tym dokumencie[94], jego celem jest wypracowanie zdolności państwa do przeciwdziałania zagrożeniom pochodzącym z cyberprzestrzeni, które mogłyby spowodować szkody dla jego interesów politycznych i gospodarczych, a także interesów obywateli i przedsiębiorców.

W *Założeniach strategii cyberbezpieczeństwa dla Rzeczypospolitej Polskiej* dokonano analizy stanu obecnego oraz przedstawiono główne założenia budowy systemu ochrony cyberprzestrzeni RP, obejmujące m.in. propozycje dotyczące jego struktury i podziału kompetencji. Równocześnie dokument zawiera wykaz niezbędnych zmian legislacyjnych oraz harmonogram opracowania *Strategii cyberbezpieczeństwa RP*, o której ostatecznym kształcie zadecyduje się w wyniku uzyskania powszechnego konsensusu wobec proponowanych rozwiązań, albowiem tylko w takim wypadku uzyska się synergię działań cząstkowych.

***

Polityka publiczna w zakresie zapewnienia cyberbezpieczeństwa jest niezwykle dynamicznym obszarem regulacji nie tylko ze względu na postęp technologiczny, powodujący pojawienie się nowych zagrożeń w cyberprzestrzeni, lecz także przez zwiększającą się intensywność ataków cybernetycznych, przynoszących poważne straty również dla instytucji unijnych i różnych struktur państwowych. Istotną rolę odgrywa też fakt, iż cyberprzestrzeń jest z założenia środowiskiem konfliktogennym, w którym potencjalnie mogą zderzać się różne interesy (w tym także narodowe), podatnym na prowadzenie działań szpiegowskich i wojennych, niemającym odporności na przeróżne manipulacje informacją, czyli tzw. cybernetyczne ataki semantyczne. Wydaje się, że podejście do tworzenia regulacji zapewniających bezpieczeństwo cyberprzestrzeni na szczeblu Unii Europejskiej i krajowym będzie ewoluowało, niemniej należy podkreślić, iż ich zaostrzenie nie przyczyni się do lepszej ochrony przed atakami, w związku z czym pożądane jest wypracowywanie kompromisu.

Bibliografia

Adamczuk M., Liedel K., *Doktryna cyberbezpieczeństwa RP*, „Przegląd Bezpieczeństwa Wewnętrznego" 2015, nr 12.

An Evaluation Framework for National Cyber Security Strategies, European Union Agency for Network and Information Security, Heraklion 2014.

[93] Zob. *Założenia strategii cyberbezpieczeństwa dla Rzeczypospolitej Polskiej*, Zespół zadaniowy, Ministerstwo Cyfryzacji, Warszawa 2016.

[94] Ibidem, s. 36.

Bayuk J.L., Healey J., Rohmeyer P., Sachs M.H., Schmidt J., Weiss J., *Cyber Security Policy Guidebook*, John Wiley & Sons Inc., Hoboken, New Jersey 2012.

Berdel-Dudzińska M., *Pojęcie cyberprzestrzeni we współczesnym polskim porządku prawnym*, „Przegląd Prawa Publicznego" 2012, nr 2.

Białoskórski R., *Cyberzagrożenia w środowisku bezpieczeństwa XXI wieku: Zarys problematyki*, Wyższa Szkoła Cła i Logistyki, Warszawa 2011.

Clark D., Berson T., Lin H.S. (Eds.), *At the Nexus of Cybersecurity and Public Policy: Some Basic Concepts and Issues*, The National Academies Press, Washington 2014.

Cyberbezpieczeństwo – problem nas wszystkich? Strategie państw UE wobec wyzwań związanych z dostępem do danych w sieci, „Raporty i Analizy Centrum Stosunków Międzynarodowych" 2015, nr 1(5).

Cybersecurity and Cyberpower: Concepts, Conditions and Capabilities for Cooperation for Action within the EU, European Parliament, Directorate-General for External policies of the Union, EXPO/B/SEDE/FWC/2009–01/LOT6/09, April 2011.

Cybersecurity in the European Union and Beyond: Exploring the Threats and Policy Responses, Directorate- General for Internal Policies, European Union, Brussels 2015.

Czyżak M., *Spamming i jego karalność w polskim systemie prawnym*, „Pomiary – Automatyka – Kontrola" 2009, nr 7(55).

EU Cybersecurity Dashboard – A Path to Secure European Cyberspace, BSA – The Software Alliance, Washington 2015.

Gadomski W., Kalinowski T., Rot M., Sadowska-Cieślak E., *Fakty i mity o TTIP: Negocjacje umowy o wolnym handlu pomiędzy Stanami Zjednoczonymi a Unią Europejską (Transatlantyckie Partnerstwo Handlowo-Inwestycyjne)*, Ministerstwo Spraw Zagranicznych, Warszawa 2015.

Grzelak M., Liedel K., *Bezpieczeństwo w cyberprzestrzeni. Zagrożenia i wyzwania dla Polski – zarys problemu*, „Bezpieczeństwo Narodowe" 2012, nr 22 (II).

Janowska A.A., *Polityka publiczna w zakresie otwartych zasobów: Unia Europejska*, Kwartalnik Kolegium Ekonomiczno-Społecznego SGH „Studia z Polityki Publicznej" 2014, nr 4(4).

Jaskiernia A., Głowacki M., *Unia Europejska i Rada Europy a kwestie ochrony praw człowieka w Internecie. Europejskie standardy zarządzania Internetem*, „Studia Medioznawcze" 2014, nr 3(58).

Kamiński F., *Problematyka neutralności sieciowej w Unii Europejskiej (zarys)*, „Telekomunikacja i Techniki Informacyjne" 2011, nr 3–4.

Kańciak A., *Problematyka cyberprzestępczości w Unii Europejskiej*, „Przegląd Bezpieczeństwa Wewnętrznego 2013, nr 8.

Karwowska K., Folga A., *Phishing: modus operandi sprawców oraz środki zapobiegawcze*, „Kortowski Przegląd Prawniczy. Czasopismo naukowe Wydziału Prawa i Administracji Uniwersytetu Warmińsko-Mazurskiego w Olsztynie" 2013, nr 4.

Nałęcz A., *Neutralność sieciowa*, „Internetowy Kwartalnik Antymonopolowy i Regulacyjny" 2015, nr 6(4).

Niedziółka T., *Regulacja Internetu a rozwój Unii Europejskiej*, Biuletyn „Opinie Fundacji Amicus Europae" 2012, nr 16.

Pietraszewska A., *Czy jest się czego obawiać, czyli o ingerencji umów ACTA i TTIP w ochronę prawa autorskiego w Sieci*, Zeszyt naukowy Naukowego Koła Cywilistów Uniwersytetu Wrocławskiego „Prawa Autorskie i Własność Przemysłowa" 2015.

Reczkowski R., Skiba A., *Bezpieczeństwo państwa w kontekście zagrożeń z cyberprzestrzeni*, w: *Innowacje i synergia w Siłach Zbrojnych RP, t. I*, red. nauk. A. Lis, R. Reczkowski, Centrum Doktryn i Szkolenia Sił Zbrojnych im. gen. broni Władysława Sikorskiego, Bydgoszcz 2012.

Rzucidło J., Węgrzyn J., *Stany nadzwyczajne w sytuacji szczególnego zagrożenia państwa w cyberprzestrzeni*, „Przegląd Prawa Konstytucyjnego 2015, nr 5(27).

Sienkiewicz P., *Analiza systemowa zagrożeń dla cyberprzestrzeni*, „Automatyka" 2009, nr 2(13).

Sienkiewicz P., Świeboda H., *Analiza systemowa bezpieczeństwa cyberprzestrzeni państwa*, „Polskie Stowarzyszenie Zarządzania Wiedzą" 2010, nr 33, seria: Studia i Materiały.

Skrzypczak J., *Polityka ochrony cyberprzestrzni RP*, „Przegląd Strategiczny" 2014, nr 7.

Tadeusiewicz R., *Zagrożenia w cyberprzestrzeni*, „Nauka" 2010, nr 4.

Vishik C., Matsubara M., Plonk A., *Key Concepts in Cyber Security: Towards a Common Policy and Technology Context for Cyber Security Norms*, w: *International Cyber Norms: Legal, Policy & Industry Perspectives*, A.-M. Maria Osula, H. Rõigas (Eds.), NATO CCD COE Publications, Tallinn 2016.

Wasilewski J., *Zarys definicyjny cyberprzestrzeni*, „Przegląd Bezpieczeństwa Wewnętrznego" 2013, nr 9.

Zelek M., *Umowa o rejestrację domeny internetowej*, C.H. Beck, Warszawa 2015.